Chapter 1
VPN Overview

A virtual private network (VPN) consists of two topological areas, the provider's network and the customer's network. The provider's network, which runs across the public Internet infrastructure, consists of routers that provide VPN services to a customer's network as well as routers that provide other services. The customer's network is commonly located at multiple physical sites. The provider's network acts to connect the various customer sites in what appears to the customer and the provider to be a private network.

To ensure that VPNs remain private and isolated from other VPNs and from the public Internet, the provider's network maintains policies that keep routing information from different VPNs separate.

A provider can service multiple VPNs as long as its policies keep routes from different VPNs separate. Similarly, a site can belong to multiple VPNs as long as it keeps routes from the different VPNs separate.

VPN Terminology

VPNs contain the following types of network devices (see Figure 1):

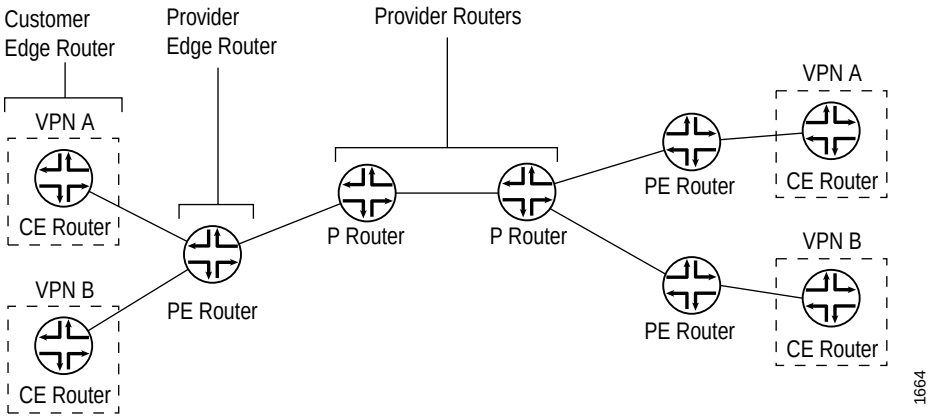
- Provider edge (PE) routers—Routers in the provider's network that connect to CE devices located at customer sites. PE routers support VPN and label functionality. (The label functionality can be provided either by RSVP or LDP.) Within a single VPN, pairs of PE routers are connected through a tunnel, which can be either an MPLS LSP or an LDP tunnel.

- Provider (P) routers—Routers within the core of the provider's network that are not connected to any routers at a customer site but that are part of the tunnel between pairs of PE routers. Provider routers support MPLS LSP or LDP functionality, but do not need to support VPN functionality.

- Customer edge (CE) devices—Routers or switches located at the customer's site that connect to the provider's network. CE devices are typically IP routers.

VPN functionality is provided by the PE routers; the provider and CE routers have no special configuration requirements for VPNs.

Figure 1: VPN Router Components



Differences between Layer 2 and Layer 3 VPNs

In a Layer 3 VPN, the routing occurs on the service provider's routers. In a Layer 2 VPN, routing occurs on the customer's routers, typically on the customer edge (CE) router. Layer 3 VPNs require more configuration on the part of the service provider, because the service provider's PE routers must know the customer's routes. Layer 2 VPNs require less configuration on the part of the service provider, because routing is handled by the customer's routers and not the service provider's.